IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter (*underlining)* and deleted subject matter *(strikethrough)*, as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of ensuring the security of a computer system comprising a host facility and a portable computing device coupled to the host facility, comprising the steps of:

loading software suitable for operating on ~~the~~ an open platform computer system in a secure environment on the open platform computer system comprising the host facility and the portable computing device;

upon loading the software on the open platform computer system, validating ~~said~~ the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in the secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the ~~desired~~ open platform computer system within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking ~~said~~ the software that is loaded as valid or invalid by the use of a flag; and,

denying ~~said~~ the software the ability to operate on any environment within ~~said~~ the open platform computer system if ~~said~~ the validator fails to identify said software as valid in order to ensure the security of ~~said~~ the open platform computer system.

2-3. (Canceled)

4. (Currently Amended) The method described in Claim 1 wherein ~~said~~ the software is supplied by a third-party source.

5. (Currently Amended) The method described in Claim 4 wherein ~~said~~ the third-party software is for execution or other use on a palmtop computer.

6. (Currently Amended) The method described in Claim 1 wherein ~~said~~ the validator program is specially constructed to reside in a secure fashion in the host facility of ~~said~~ the open platform computer system.

7. (Currently Amended) The method described in Claim 1 wherein ~~said~~ the method operates on a computer system which comprises:

a host computer; and

a portable computing device coupled to ~~said~~ the host computer and wherein the validating operation is performed by the host computer for the portable computing device.

8. (Currently Amended) An apparatus for ensuring the security of an open platform computer system, comprising:

a portable computing device coupled to a host computer, wherein ~~said~~ the portable computing device is configured to load software from ~~said~~ the host computer to ~~said~~ the portable computing device for operating on ~~said~~ the portable computing device; and,

a validation program residing on the computer system in a secure fashion that is configured for:

validating ~~said~~ the software by first scanning ~~said~~ the software that is loaded in a secure environment;

wherein the act of scanning and validating comprises running the code in an emulator for the ~~desired~~ open platform computer system within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking ~~said~~ the software as valid or invalid by the use of a flag; and,

denying ~~said~~ the software the ability to operate in any environment on ~~said~~ the computer system if ~~said~~ the validator fails to identify ~~said~~ the software as valid in order to ensure the security of ~~said~~ the computer system.

9. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the host computer is coupled to a network.

10. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the portable computing device is a handheld computing device.

11. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the portable computing device is a personal data assistant.

12. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the portable computing device is coupled to ~~said~~ the host computer by an infrared device.

13. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the portable computing device is coupled to said host computer by an RF enabled device

14. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the validation program resides in ~~said~~ the host computer of the computer system in a fashion intended to be secure.

15. (Currently Amended) The apparatus described in Claim 8 wherein ~~said~~ the validation program is configured to evaluate third-party software and attach a digital "valid" flag if ~~said~~ the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to ~~said~~ the third-party software in ~~said~~ the third-party software is not found to be clean of known security compromising routines.

16. (Currently Amended) The apparatus described in Claim 15 wherein ~~said~~ the portable computing device is configured to load third-party software files with ~~said~~ the digital

"valid" flag attached and to refrain from loading third-party software files which have no flag attached or have ~~said~~ the "invalid" flag attached..

17. (Currently Amended) The apparatus described in Claim 15 wherein ~~said~~ the portable computing device is a Personal Data Assistant.

18. (Currently Amended) An apparatus for ensuring the security of an open platform computer system, comprising:

a handheld computing device coupled to a network, wherein ~~said~~ the handheld computing device is configured to load software from ~~said~~ the network to ~~said~~ the handheld computing device for operation on ~~said~~ the handheld computing device; and,

a validation program that resides on the network that is configured for:

validating ~~said~~ the software by scanning ~~the~~ files of ~~said~~ the software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld computing device;

wherein the act of scanning and validating comprises running ~~the~~ code of the software in an emulator for the ~~desired~~ open platform computer system within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures;

marking ~~said~~ the software as valid or invalid by the use of a flag; and,

denying ~~said~~ the software the ability to operate on any environment on ~~said~~ the computer system if said validator fails to identify ~~said~~ the software as valid in order to ensure the security of ~~said~~ the computer system.

19. (Currently Amended) The apparatus described in Claim 18 wherein ~~said~~ the validation program resides in ~~said~~ the network in a fashion intended to be secure.

20. (Currently Amended) The apparatus described in Claim 18, wherein ~~said~~ the handheld computing device is configured to load third-party software files with ~~said~~ the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have ~~said~~ the "invalid" flag attached.

21. (Currently Amended) The apparatus described in Claim 18 wherein ~~said~~ the validation program is configured to evaluate third-party software and attach a digital "valid" flag if ~~said~~ the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to ~~said~~ the third-party software in ~~said~~ the third-party software is not found to be clean of known security compromising routines.

22-28. (Withdrawn)